Abstract of Cited Ref. 4

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-067268**
(43)Date of publication of application : **16.03.2001**

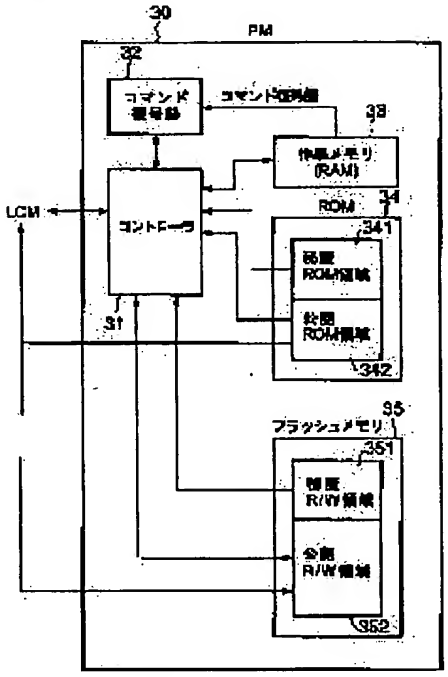
(51)Int.Cl. G06F 12/14
H04L 9/36
H04N 7/16

(21)Application number : **11-237274**
(22)Date of filing : **24.08.1999**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **KAMIBAYASHI TATSU**
TAMURA MASABUMI

(54) METHOD FOR MANAGING CONTENTS, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To make preventable the failure of security due to the alteration of a secret region operation command.
SOLUTION: At the time of issuing a desired secret region operation command from an LCM to be realized on a PC for operating a secret R/W region 351 ensured so that its boundary can be brought into contact with a public R/W region 352 on a memory 35, the whole command or the parameter part of the command is enciphered, and the enciphered secret region operation command is transmitted to a PM 30 side. At the time of receiving the secret region operation command, a controller 31 of the PM 30 allows a command decoding part 32 to decode the whole command or the parameter part of the command, and the secret R/W region 351 is operated according to the decoded secret region operation command. In this case, when the command is a CHANGE command for changing the secret R/W region 351, the controller 31 deletes the data of the reduced/enlarged part of the secret R/W region 351 at the time of changing the secret R/W region 351.



Cited Ref. 4

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－67268
（P2001－67268A）
(43)公開日　平成13年３月16日(2001.3.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｈ０４Ｌ　9/36		Ｈ０４Ｎ　7/16	Ｚ	５Ｃ０６４
Ｈ０４Ｎ　7/16		Ｈ０４Ｌ　9/00	６８５	５Ｊ１０４

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－237274

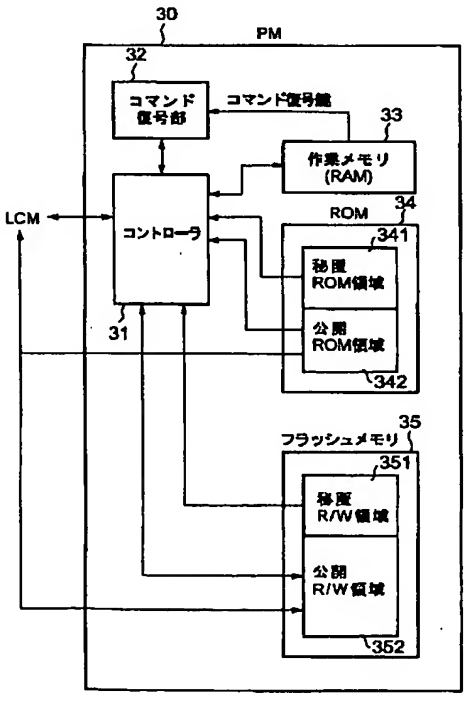
(22)出願日　平成11年８月24日(1999.8.24)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　田村　正文
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　コンテンツ管理方法及び記憶媒体

(57)【要約】
【課題】秘匿領域操作コマンドの改ざんによるセキュリティの破綻を防ぐ。
【解決手段】メモリ３５上に公開Ｒ／Ｗ領域３５２と境界を接するように確保された秘匿Ｒ／Ｗ領域３５１を操作するために、ＰＣ上に実現されるＬＣＭから所望の秘匿領域操作コマンドを発行する際には、コマンド全体または当該コマンドのパラメータ部分を暗号化し、その暗号化された秘匿領域操作コマンドをＰＭ３０側に送る。ＰＭ３０のコントローラ３１は、この秘匿領域操作コマンドを受け取った場合、コマンド復号部３２により、当該コマンドのコマンド全体またはパラメータ部分を復号させ、この復号された秘匿領域操作コマンドに従って秘匿Ｒ／Ｗ領域３５１を操作する。ここで、上記コマンドが秘匿Ｒ／Ｗ領域３５１を変更するＣＨＡＮＧＥコマンドの場合、コントローラ３１はその領域変更に際し、秘匿Ｒ／Ｗ領域３５１の縮小／拡大部分のデータを消去する。



1

【特許請求の範囲】

【請求項１】　デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理方法であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化し、

前記記憶媒体側では、前記コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、

この復号された秘匿領域操作コマンドに従って前記秘匿領域を操作することを特徴とするコンテンツ管理方法。

【請求項２】　記憶媒体上の所定のメモリ領域を分割することにより、デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と境界を接して確保された、前記コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理方法であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化し、

前記記憶媒体側では、前記コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、

この復号された秘匿領域操作コマンドに従って前記秘匿領域を操作し、当該コマンドが前記秘匿領域のサイズの変更を指示する特定秘匿領域操作コマンドの場合には、前記秘匿領域と前記公開領域との境界を移動することで前記秘匿領域のサイズを変更し、少なくとも前記秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去することを特徴とするコンテンツ管理方法。

【請求項３】　デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域を、専用のコマンドである秘匿領域操作コマンドによって操作するコンテンツ管理装置であって、

前記記憶媒体に対する所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化するコマンド暗号化手段と、

前記コマンド暗号化手段により前記コマンド全体または

2

パラメータ部分が暗号化された秘匿領域操作コマンドを前記記憶媒体側に送信する送信手段とを具備することを特徴とするコンテンツ管理装置。

【請求項４】　デジタル・コンテンツが記録される記憶媒体において、

前記記憶媒体に記録されたコンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域が確保されるメモリと、

前記秘匿領域を操作するための専用のコマンドであり、そのコマンド全体または当該コマンドのパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合に、この暗号化された秘匿領域操作コマンドのコマンド全体またはパラメータ部分を復号するコマンド復号手段と、

前記コマンド復号手段により復号された秘匿領域操作コマンドに従って前記秘匿領域を操作するコントローラとを具備することを特徴とする記憶媒体。

【請求項５】　デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と、前記公開領域に記録されたコンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される、特定手続にてのみアクセスが可能な秘匿領域とが境界を接して確保されたメモリと、

前記秘匿領域を操作するための専用のコマンドであり、そのコマンド全体または当該コマンドのパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合に、この暗号化された秘匿領域操作コマンドのコマンド全体またはパラメータ部分を復号するコマンド復号手段と、

前記コマンド復号手段により復号された秘匿領域操作コマンドに従って前記秘匿領域を操作するコントローラであって、当該コマンドが前記秘匿領域のサイズの変更を指示する特定秘匿領域操作コマンドの場合には、前記秘匿領域と前記公開領域との境界を移動することで前記秘匿領域のサイズを変更し、少なくとも前記秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去するコントローラとを具備することを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像データや音楽データに代表される種々のデジタル・コンテンツの著作権保護を図るのに好適なコンテンツ管理方法及び記憶媒体に関する。

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メデ

ィアに格納された画像データや音楽データなど様々なデジタル・コンテンツを再生できるほか、インターネット等を通じてデジタル・コンテンツをダウンロードして使用することもできる。

【０００３】これらのデジタル・コンテンツは、例えばＭＰＥＧ２、ＭＰ３といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタル・コンテンツを不正使用から保護するための技術の必要性が叫ばれている。特に、メモリカードのように別の機器に移動しても記録／再生できるリムーバブルな記憶媒体は、その仕様が基本的にはオープンであり、コンテンツの移動／コピーを自由に行うことができるので、その記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護できるようにすることは重要である。

【０００４】そこで、メモリカードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。ここでは、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際に、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを復号するためのコンテンツ復号鍵）の暗号化／復号化またはコンテンツの暗号化／復号化に用いることが考えられている。

【０００５】

【発明が解決しようとする課題】さて、デジタル・コンテンツを利用するアプリケーションを搭載した機器（以下、ホストと称する）では、上述の著作権保護の観点から、記憶媒体（メモリカード等の記憶メディア部とコントローラとが一体化された記憶媒体）の秘匿領域に格納されているコンテンツキー（コンテンツ復号鍵）などを、確実に上書きしたり消去したりすることが必要となる。

【０００６】ところが従来の記憶媒体の秘匿領域に対する書き込みや消去のコマンド（秘匿領域操作コマンド）には、そのコマンド全体、或いはそのコマンドのパラメータの改ざんに対して何ら考慮されていなかった。このため、ホストと記憶媒体との間の通信を傍受してコマンドを改ざんし、記憶媒体の秘匿領域に格納されている特定のデータの消去を阻害するなど、セキュリティに対する攻撃が存在する虞がある。

【０００７】本発明は上記事情を考慮してなされたものでその目的は、秘匿領域を対象とする操作を指示するコマンド（秘匿領域操作コマンド）の改ざんによるセキュリティの破綻を防ぐことができるコンテンツ管理方法及び記憶媒体を提供することにある。

【０００８】

【課題を解決するための手段】本発明は、デジタル・コンテンツが記録される記憶媒体に確保された、当該コンテンツを復号するのに必要なコンテンツ復号鍵を含む情報が記録される秘匿領域を操作するために、所望のタイプの秘匿領域操作コマンドを発行するに際し、当該コマンド全体または当該コマンドのパラメータ部分を暗号化して、しかる後に、この暗号化された秘匿領域操作コマンドを記憶媒体側に送るようにする一方、記憶媒体側では、コマンド全体またはパラメータ部分が暗号化された秘匿領域操作コマンドを受け取った場合、当該コマンドのコマンド全体またはパラメータ部分を復号し、この復号された秘匿領域操作コマンドに従って秘匿領域を操作することを特徴とする。ここで、秘匿領域操作コマンドのコマンド全体またはパラメータ部分の暗号化に用いる暗号鍵と、秘匿領域操作コマンドの暗号化されたコマンド全体または暗号化されたパラメータ部分の復号に用いる復号鍵とは、暗号化側と復号化側との間の通信を通じて、相互に共有する鍵生成のアルゴリズムに従い生成すればよい。また、この鍵生成は、秘匿領域操作コマンドの送信の都度、その送信に先立って行われるようにするとよい。

【０００９】このように、記憶媒体のメモリ領域に確保された秘匿領域を対象とする秘匿領域操作コマンドのコマンド全体またはパラメータ部分を暗号化して当該記憶媒体に送り、当該記憶媒体ではそれを復号化して実行することで、コマンド改ざんにより秘匿領域の特定のデータの消去が阻害されるといった、セキュリティの破綻を防ぐことができる。

【００１０】ここで、秘匿領域操作コマンド全体を暗号化した場合には、そのパラメータ部分で指定されるメモリ領域上の位置や操作の対象となるサイズを改ざんすることが極めて困難となるだけでなく、コマンドの同定すら困難となる。一方、秘匿領域操作コマンドのパラメータ部分だけを暗号化した場合には、ＯＰコード部分は暗号化されていないため、記憶媒体側では秘匿領域操作コマンドを受信した際に、直ちに当該コマンドの解釈処理に入ることができるため、パラメータ部分で指定されるメモリ領域上の位置や操作の対象となるサイズを改ざんすることを防止しながら、記憶媒体側での動作（処理の割当て）の最適化を図ることができる。

【００１１】また本発明は、上記記憶媒体上の所定のメモリ領域を分割して、デジタル・コンテンツが記録される、通常手続でアクセスが可能な公開領域と、上記の秘

匿領域とを、境界を接するようにして確保する一方、上記秘匿領域操作コマンドの１つとして、秘匿領域のサイズの変更指示が可能な特定秘匿領域操作コマンド（ＣＨＡＮＧＥコマンド）が利用可能なようにし、記憶媒体側で復号された秘匿領域操作コマンドが特定秘匿領域操作コマンドの場合には、秘匿領域と公開領域との境界を移動することで秘匿領域のサイズを変更し、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータを消去するようにしたことをも特徴とする。

【００１２】本発明においては、秘匿領域操作コマンドの改ざんを防ぎながら、当該コマンドとして特定秘匿領域操作コマンドを使用した場合には、秘匿領域と公開領域とのサイズの比率を変更すること、即ち秘匿領域を縮小すると共にその縮小分だけ公開領域を拡大すること、或いは秘匿領域を拡大すると共にその拡大分だけ公開領域を縮小することができる。これにより記憶媒体を、例えば、１コンテンツ当たりのデータサイズが大きくなるビデオデータの記憶に用いるような場合には、扱える総コンテンツサイズを重視して秘匿領域を縮小すると共に公開領域を拡大し、１コンテンツ当たりのデータサイズが小さくて済む音楽データの記憶に用いる場合には、扱える総コンテンツ数を重視して秘匿領域を拡大すると共に公開領域を縮小するといったことが可能となる。

【００１３】しかも本発明においては、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータ、即ち秘匿領域と公開領域との現在の境界（変更前の境界）と変更後の境界との間のデータが自動的に消去されることから、秘匿領域の縮小変更に伴ってその秘匿領域の縮小部分が公開領域に加えられたとしても、その縮小部分に記憶されていた秘密のデータが漏洩する虞はない。ここで、秘匿領域が拡大変更される場合にも、その変更部分のデータが自動的に消去されるようにするとよい。この場合、公開領域のうち、秘匿領域との境界の領域部分に所望のデータを書き込んだ後、秘匿領域操作コマンドを用いて当該領域部分が秘匿領域側に入るように秘匿領域を拡大変更することで、その拡大部分の本来秘匿されるべきデータを自由に利用可能にしようとする「攻撃」がなされても、対抗できる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態につき図面を参照して説明する。図１は本発明の一実施形態に係るコンテンツ利用管理システムの構成を主として示すブロック図である。

【００１５】コンテンツ利用管理システム（以下、ＬＣＭ（Licence (SDMI-)Compliant Module）と称する）１０は、メモリカード等の記憶メディア（以下、ＰＭ（Portable Memory）と称する）３０に記録できる複製コンテンツの数を規制し、当該ＰＭ３０に記録された複製コンテンツの記録、再生等を行うもので、例えば、パーソナルコンピュータ（以下、ＰＣと称する）１上で実行可能なソフトウェアとして実現されている。

【００１６】ＬＣＭ１０は、コンテンツ配信サーバ等から配信される暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツの復号鍵）などを受信する機能を有する。

【００１７】ＬＣＭ１０は、当該ＬＣＭ１０の中枢をなすセキュア・コンテンツ・サーバ１１を有している。セキュア・コンテンツ・サーバ１１は、ＬＣＭ１０で受信される、利用者が購入した暗号化コンテンツを図示せぬデータ格納部に格納し、その復号鍵（コンテンツ復号キー）を図示せぬライセンス格納部に格納する。なお、受信された暗号化コンテンツは、一旦復号され、しかる後に形式変換や再暗号化が施されることが多い。このセキュア・コンテンツ・サーバ１１が管理するコンテンツは、当該サーバ１１によりＬＣＭ１０上で再生することも可能である。

【００１８】セキュア・コンテンツ・サーバ１１はまた、メディアＩ／Ｆ部１３に装着可能なＰＭ３０に対してコンテンツデータ（デジタル・コンテンツ）を当該Ｉ／Ｆ部１３経由で出力する機能を有している。このＰＭ３０は、専用の記録再生装置（以下、簡単にＰＤ（Portable Device）と称する）２０にセットして用いることで、当該ＰＭ３０に記録されたコンテンツをＰＤ２０上で再生することもできる。セキュア・コンテンツ・サーバ１１は、ＰＤ２０にセットされたＰＭ３０に対し、ＰＤ　Ｉ／Ｆ部１２及びＰＤ２０経由で出力する機能も有する。つまり、セキュア・コンテンツ・サーバ１１からＰＭ３０へのコンテンツの記録は、メディアＩ／Ｆ部１３を通じて直接行われるか、またはＰＤ　Ｉ／Ｆ部１２及びＰＤ２０を経由して行われる。

【００１９】Ｉ／Ｆ部１２，１３は、それぞれセキュア・コンテンツ・サーバ１１から当該Ｉ／Ｆ部１２，１３を介してＰＭ３０側に送られる特定コマンドである秘匿Ｒ／Ｗ領域操作コマンド（後述する秘匿Ｒ／Ｗ領域３５１を対象とする操作を指示するコマンド）を暗号化するコマンド暗号化部１２０，１３０を有している。

【００２０】セキュア・コンテンツ・サーバ１１は更に、ＰＣ１の入出力装置（図示せず）からの入力を受け付けるユーザＩ／Ｆ部１４を有している。ユーザがキーボード、マウス等の入力装置を操作して入力した指示は、このユーザＩ／Ｆ部１４で受け付けられてセキュア・コンテンツ・サーバ１１に渡される。この指示には、後述する秘匿Ｒ／Ｗ領域３５１の大きさの変更指示も含まれる。

【００２１】図２は、ＰＭ３０の構成を示す。同図に示すように、ＰＭ３０は、ＬＣＭ１０から直接にまたはＰＤ２０を介して送られるコマンドを解釈・実行するコントローラ３１と、暗号化されたコマンドを復号するコマ

ンド復号部３２と、コントローラ３１とコマンド復号部３２によってのみアクセスが可能な、例えばＲＡＭにより構成される作業メモリ３３と、読み出し専用の不揮発性メモリとしてのＲＯＭ３４と、書き換え可能な不揮発性メモリとしてのフラッシュメモリ３５とを備えている。

【００２２】ＲＯＭ３４の記憶領域は、コントローラ３１を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない読み出し専用の記憶領域（以下、秘匿ＲＯＭ領域と称する）３４１と、通常の手順にてアクセス可能な読み出し専用の記憶領域（以下、公開ＲＯＭ領域と称する）３４２とに割り当てられている。

【００２３】秘匿ＲＯＭ領域３４１には、対応するＰＭ３０に固有の秘密情報である秘匿メディアＩＤ等の定数が予め記憶される。一方、公開ＲＯＭ領域３４２には、対応するＰＭ３０の識別情報としてのメディアＩＤ、デジタル・コンテンツの記録または再生のためのアクセス要求を無効化すべき機器（ＬＣＭ、ＰＤ）を表す情報等が記憶される。

【００２４】次に、フラッシュメモリ３５の記憶領域は、コントローラ３１を通して非公開の手順でしかアクセスできない記憶領域（以下、秘匿Ｒ／Ｗ領域と称する）３５１と、通常の手順にてアクセス可能な記憶領域（以下、公開Ｒ／Ｗ領域と称する）３５２とに割り当てられている。

【００２５】公開Ｒ／Ｗ領域３５２には、暗号化されたコンテンツ・データ（暗号化コンテンツ）が記憶される。一方、秘匿Ｒ／Ｗ領域３５１には、公開Ｒ／Ｗ領域３５２に記憶されるコンテンツ・データに対応する、当該コンテンツ・データを復号するためのコンテンツキー（コンテンツ復号鍵）が記憶される。秘匿Ｒ／Ｗ領域３５１にはまた、当該秘匿Ｒ／Ｗ領域３５１の開始アドレスとサイズの情報が記憶される。この情報は、秘匿Ｒ／Ｗ領域３５１の終了アドレス側の所定位置に記憶される。ここで用いられるアドレスは、特に断らない限り、メモリの物理アドレスではなくて、そのメモリが割り当てられるアドレス空間のアドレスを表す。

【００２６】図３は、フラッシュメモリ３５の記憶領域のメモリマップの一例を示す。同図に示すように、本実施形態では、秘匿Ｒ／Ｗ領域３５１はフラッシュメモリ３５の記憶領域の高アドレス側に割り当てられ、公開Ｒ／Ｗ領域３５２は同じく低アドレス側に割り当てられている。ここで、秘匿Ｒ／Ｗ領域３５１の終了アドレスはフラッシュメモリ３５の最終物理アドレスが割り当てられるメモリアドレス空間のアドレスに一致し、公開Ｒ／Ｗ領域３５２の開始アドレスはフラッシュメモリ３５の先頭物理アドレス（０番地）が割り当てられるメモリアドレス空間のアドレスに一致する。また、秘匿Ｒ／Ｗ領域３５１の開始アドレスは、公開Ｒ／Ｗ領域３５２の終了アドレスに一致する。本実施形態では、この秘匿Ｒ／Ｗ領域３５１の開始アドレス（＝公開Ｒ／Ｗ領域３５２の終了アドレス）、つまり秘匿Ｒ／Ｗ領域３５１と公開Ｒ／Ｗ領域３５２との境界を、ユーザの指示に応じてＬＣＭ１０側から発行されるＣＨＡＮＧＥコマンド（秘匿Ｒ／Ｗ領域変更命令）と呼ぶ専用のコマンド（命令）の実行により指定サイズだけ可変できるようになっている。

【００２７】図４は、ＬＣＭ１０からＰＭ３０に対して発行される秘匿Ｒ／Ｗ領域操作コマンド（秘匿領域操作コマンド）の形式を示す。

【００２８】ここでは、各秘匿Ｒ／Ｗ領域操作コマンド（コマンドデータ）は、ＳＥＮＤと呼ばれる送信命令でＰＭ３０側に送られる。このコマンドデータは、先頭から順に、秘匿Ｒ／Ｗ領域操作の種別、つまりコマンド種別を示すコマンドコードとしてのＯＰコードと、秘匿Ｒ／Ｗ領域操作の対象となる記憶領域（秘匿Ｒ／Ｗ領域３５１内の領域）の開始位置のアドレス空間上のアドレス（開始アドレス）を示すＡＤＤＲＥＳＳと、秘匿Ｒ／Ｗ領域操作の対象となる領域サイズを例えばバイト単位で示すＬＥＮＧＴＨとから構成される。本実施形態において、ＯＰコードは１バイト、ＡＤＤＲＥＳＳは４バイト、そしてＬＥＮＧＴＨは２バイトで、それぞれ表現される。コマンドデータのうち、ＯＰコードを除くデータを、オペランド或いはパラメータと呼ぶ。また、本実施形態で適用される秘匿Ｒ／Ｗ領域操作コマンドには、前記したＣＨＡＮＧＥコマンド（秘匿Ｒ／Ｗ領域変更命令）の他に、秘匿Ｒ／Ｗ領域３５１の指定領域からのデータ読み出しを指示するＲＥＡＤコマンド（秘匿Ｒ／Ｗ領域読み出し命令）、秘匿Ｒ／Ｗ領域３５１の指定領域へのデータ書き込みを指示するＷＲＩＴＥコマンド（秘匿Ｒ／Ｗ領域書き込み命令）、秘匿Ｒ／Ｗ領域３５１内の指定領域のデータ消去を指示するＥＲＡＳＥコマンド（秘匿Ｒ／Ｗ領域消去命令）がある。

【００２９】次に、本実施形態の動作を、図５乃至図７のフローチャートを参照して説明する。まず、ＬＣＭ１０のセキュア・コンテンツ・サーバ１１からメディアＩ／Ｆ部１３（またはＰＤ　Ｉ／Ｆ部１２）に対して、ＰＭ３０への秘匿Ｒ／Ｗ領域操作コマンドの送信が要求され、対応するコマンドデータが渡されたものとする。すると、Ｉ／Ｆ部１３（または１２）は、セキュア・コンテンツ・サーバ１１から渡されたコマンドデータ全体、つまりＯＰコード（１バイト）、ＡＤＤＲＥＳＳ（４バイト）、及びＬＥＮＧＴＨ（２バイト）の合計７バイトのコマンドデータを、ＬＣＭ１０が有するコマンド暗号化鍵を用いてコマンド暗号化部１３０（または１２０）により暗号化し、その暗号化されたコマンドデータをＳＥＮＤ命令により、そのまま（またはＰＤ２０を介して）ＰＭ３０のコントローラ３１に送信する（ステップＳ１）。

【００３０】ＰＭ３０内のコントローラ３１は、ＬＣＭ

１０側から送られた暗号化コマンドを受け取ると、その暗号化コマンドをコマンド復号部３２に渡して、復号を要求する（ステップＳ２）。

【００３１】するとコマンド復号部３２は、コントローラ３１から渡された暗号化コマンドを、当該コマンドの暗号化に用いられたコマンド暗号鍵に対応して生成されたコマンド復号鍵で復号する（ステップＳ３）。このコマンド復号鍵は、例えば、対応する秘匿Ｒ／Ｗ領域操作コマンドの送信に先立って行われる、ＬＣＭ１０とＰＭ３０のコントローラ３１との間の通信を通じて、相互に共有する鍵生成のアルゴリズムに従いコントローラ３１により生成される。生成されたコマンド復号鍵はＰＭ３０の作業メモリ３３に格納される。一方、このコマンド復号鍵に対応するコマンド暗号鍵は、ＬＣＭ１０のセキュア・コンテンツ・サーバ１１にて生成される。

【００３２】コマンド復号部３２は、暗号化コマンドを復号すると、その復号されたコマンド、つまり平文のコマンドをコントローラ３１に返す（ステップＳ４）。これによりコントローラ３１は、コマンド復号部３２から返されたコマンド（復号された秘匿Ｒ／Ｗ領域操作コマンド）のＯＰコードを解釈して、そのコマンド種別（命令種別）を判断する（ステップＳ５）。

【００３３】もし、ＯＰコードがＲＥＡＤコマンド（秘匿Ｒ／Ｗ領域読み出し命令）を指定しているならば（ステップＳ６）、コントローラ３１は当該ＲＥＡＤコマンドのパラメータ（オペランド）ＡＤＤＲＥＳＳ，ＬＥＮＧＴＨに従って、ＡＤＤＲＥＳＳで指定される秘匿Ｒ／Ｗ領域３５１の位置からＬＥＮＧＴＨバイトのデータを読み出し（ステップＳ７）、その読み出したデータをＬＣＭ１０に転送して動作（ＲＥＡＤコマンドの実行）を終了する（ステップＳ８）。

【００３４】また、ＯＰコードがＷＲＩＴＥコマンド（秘匿Ｒ／Ｗ領域書き込み命令）を指定しているならば（ステップＳ９）、コントローラ３１は当該ＷＲＩＴＥコマンドのパラメータＡＤＤＲＥＳＳ（アドレス），ＬＥＮＧＴＨ（データ長）を作業メモリ３３に一旦格納する（ステップＳ１０）。このステップＳ１０の処理により、ＷＲＩＴＥコマンドに続いてＬＣＭ１０側から転送される書き込みデータの格納先（の開始位置）とデータ長を示す情報が作業メモリ３３に保持される。

【００３５】コントローラ３１は、ステップＳ１０を実行すると、ＬＣＭ１０から転送される書き込みデータを受け取る（ステップＳ１１）。そしてＬＣＭ１０は、受け取った書き込みデータを、先のステップＳ１０で作業メモリ３３に格納したＷＲＩＴＥコマンドのパラメータＡＤＤＲＥＳＳ，ＬＥＮＧＴＨに従って、ＡＤＤＲＥＳＳで指定される秘匿Ｒ／Ｗ領域３５１の位置からＬＥＮＧＴＨバイトだけ書き込んで動作（ＷＲＩＴＥコマンドの実行）を終了する（ステップＳ１２）。

【００３６】また、ＯＰコードがＥＲＡＳＥコマンド（消去命令）を指定しているならば（ステップＳ１３）、コントローラ３１は当該ＥＲＡＳＥコマンドのパラメータＡＤＤＲＥＳＳ，ＬＥＮＧＴＨに従って、ＡＤＤＲＥＳＳで指定される秘匿Ｒ／Ｗ領域３５１の位置からＬＥＮＧＴＨで指定されるデータ長（バイト長）だけ、該当するデータを消去して動作（ＥＲＡＳＥコマンドの実行）を終了する（ステップＳ１４）。ここでのデータ消去は、該当する領域に、所定のデータ、例えば０を書き込むことにより、つまり該当する領域のデータを０で置換えることにより行われる。

【００３７】また、ＯＰコードがＣＨＡＮＧＥコマンド（秘匿Ｒ／Ｗ領域変更命令）を指定しているならば（ステップＳ１５）、コントローラ３１は当該ＣＨＡＮＧＥコマンド中のＡＤＤＲＥＳＳ（つまり変更指定された秘匿Ｒ／Ｗ領域３５１の開始アドレス）と、秘匿Ｒ／Ｗ領域３５１の所定位置に記憶されている当該秘匿Ｒ／Ｗ領域３５１の開始アドレス（つまり現在の秘匿Ｒ／Ｗ領域３５１の開始アドレス）とを比較することで、秘匿Ｒ／Ｗ領域３５１の縮小が指定されているのか否か（つまり拡大が指定されているのか）を判定する（ステップＳ１６）。

【００３８】もし、秘匿Ｒ／Ｗ領域３５１の指定開始アドレスが現開始アドレスより大きいならば、コントローラ３１は秘匿Ｒ／Ｗ領域３５１の縮小が指定されていると判定し、フラッシュメモリ３５の現開始アドレスからＣＨＡＮＧＥコマンド中のＬＥＮＧＴＨの示すデータ長だけ（つまり上記指定開始アドレスまで）該当するデータを消去する（ステップＳ１７）。そしてコントローラ３１は、秘匿Ｒ／Ｗ領域３５１の開始位置（秘匿Ｒ／Ｗ領域３５１と公開Ｒ／Ｗ領域３５２との境界位置）をＣＨＡＮＧＥコマンド中のＡＤＤＲＥＳＳの指定する位置に変更して、当該秘匿Ｒ／Ｗ領域３５１をＣＨＡＮＧＥコマンド中のＬＥＮＧＴＨの指定するサイズだけ縮小すると同時に、同サイズだけ公開Ｒ／Ｗ領域３５２を拡大し、動作（ＣＨＡＮＧＥコマンドの実行）を終了する（ステップＳ１８）。このステップＳ１８の処理は、秘匿Ｒ／Ｗ領域３５１の終了アドレス側の所定位置に格納されている、当該秘匿Ｒ／Ｗ領域３５１の開始アドレスとサイズの情報を、当該秘匿Ｒ／Ｗ領域３５１の縮小後の情報に書き換えることで実現される。

【００３９】これに対し、秘匿Ｒ／Ｗ領域３５１の指定開始アドレスが現開始アドレスより小さいならば、コントローラ３１は秘匿Ｒ／Ｗ領域３５１の拡大が指定されていると判定し、フラッシュメモリ３５の上記指定開始アドレス（ＣＨＡＮＧＥコマンド中のＡＤＤＲＥＳＳで指定されるフラッシュメモリ３５のアドレス）から当該ＣＨＡＮＧＥコマンド中のＬＥＮＧＴＨの示すデータ長だけ（つまり上記現開始アドレスまで）該当するデータを消去する（ステップＳ１９）。そしてコントローラ３１は、秘匿Ｒ／Ｗ領域３５１の開始位置をＣＨＡＮＧＥ

コマンド中のＡＤＤＲＥＳＳの指定する位置に変更して、当該秘匿Ｒ／Ｗ領域３５１をＣＨＡＮＧＥコマンド中のＬＥＮＧＴＨの指定するサイズだけ拡大すると同時に、同サイズだけ公開Ｒ／Ｗ領域３５２を縮小し、動作（ＣＨＡＮＧＥコマンドの実行）を終了する（ステップＳ２０）。このステップＳ２０の処理は、秘匿Ｒ／Ｗ領域３５１の終了アドレス側の所定位置に格納されている、当該秘匿Ｒ／Ｗ領域３５１の開始アドレスとサイズの情報を、当該秘匿Ｒ／Ｗ領域３５１の拡大後の情報に書き換えることで実現される。

【００４０】図８に、秘匿Ｒ／Ｗ領域３５１の開始アドレスがＡＤ１の状態で、ＣＨＡＮＧＥコマンドによりＡＤ２（但し、ＡＤ２＞ＡＤ１）に変更することが指定された場合の、当該ＣＨＡＮＧＥコマンド実行後のフラッシュメモリ３５のメモリマップを示す。ここでは、フラッシュメモリ３５内のＡＤ１～ＡＤ２までの領域３５３のデータが上記ステップＳ１７にて消去される。そして、この領域３５３の分だけ、秘匿Ｒ／Ｗ領域３５１は縮小され、公開Ｒ／Ｗ領域３５２は拡大される。

【００４１】以上、秘匿Ｒ／Ｗ領域操作コマンドをＯＰコードを含めて暗号化して（つまりコマンドデータ全体を暗号化して）、ＳＥＮＤ命令によりＬＣＭ１０（内のメディアＩ／Ｆ部１３またはＰＤ　Ｉ／Ｆ部１２）からＰＭ３０側に送る場合について説明したが、これに限るものではない。例えば、図９の形式のコマンド（命令）を用い、コマンドデータ中のＯＰコードは、暗号化せずに、パラメータ（オペランド）だけを暗号化して、そのパラメータのみが暗号化されたコマンドデータ自体をＬＣＭ１０からＰＭ３０側へ送るようにしても構わない。

【００４２】この場合の、ＰＭ３０の動作を簡単に説明する。

【００４３】まずコントローラ３１は、ＬＣＭ１０からパラメータのみが暗号化された図９の形式の暗号化コマンドを受け取ると、そのコマンド中の暗号化されていないＯＰコードを解釈し、その解釈結果に応じてＰＭ３０の動作（処理の割当て）の最適化を図る。

【００４４】ＯＰコードのサイズは１バイトであり、短いデータである。しかし、先の例のように当該ＯＰコードも暗号化されている場合、当該ＯＰコードも復号する必要があり、その復号に一定のオーバヘッドを要する。

【００４５】ところが、ＯＰコードの暗号化を行わないならば、ＬＣＭ１０からコマンドを受け取った段階で直ちにＯＰコードの解釈が実行できるため、上記の如くＰＭ３０の動作を最適化することができる。即ちコントローラ３１は、ＯＰコードの解釈により、受信コマンドが秘匿Ｒ／Ｗ領域操作コマンドのうちのＲＥＡＤコマンド、ＷＲＩＴＥコマンド、ＥＲＡＳＥコマンド、またはＣＨＡＮＧＥコマンドのいずれであるかを判定すると、直ちに判定したコマンドの実行シーケンスに入る。そしてコントローラ３１は、この実行シーケンスの中で、受信コマンド中のＯＰコードを除く部分、つまり暗号化されたパラメータ（オペランド）をコマンド復号部３２に渡して、復号を要求する。

【００４６】コマンド復号部３２は、コントローラ３１から渡された暗号化パラメータ（オペランド）を復号する。このコマンド復号部３２の復号動作は、復号対象が暗号化パラメータである点を除け、先の暗号化コマンドの復号の場合と同様である。コマンド復号部３２は、暗号化パラメータを復号すると、その復号されたパラメータ、つまり平文のパラメータ（オペランド）をコントローラ３１に返す。

【００４７】コントローラ３１は、上記実行シーケンスの中でコマンド復号部３２から平文のパラメータを受け取ると、そのパラメータに従って、そのシーケンスに固有の動作、即ち先に解釈したコマンドの指示する動作を行う。

【００４８】

【発明の効果】以上詳述したように本発明によれば、デジタル・コンテンツの記録再生に利用される記憶媒体に確保された秘匿領域を操作するための秘匿領域操作コマンドの全体またはパラメータ部分を暗号化して当該記憶媒体に送り、当該記憶媒体ではそれを復号化して実行するようにしたので、秘匿領域操作コマンドの改ざんによるセキュリティの破綻を防ぐことができる。

【００４９】また本発明によれば、記憶媒体のメモリ領域上に連続的に確保された秘匿領域と公開領域との境界を特定秘匿領域操作コマンドにより移動して秘匿領域と公開領域のサイズの比率を変更できるだけでなく、少なくとも秘匿領域が縮小変更される場合は、その秘匿領域変更に際してその変更部分のデータが自動的に消去されるため、秘匿されたデータが漏洩するのを防止できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンテンツ利用管理システムの構成を主として示すブロック図。

【図２】図１中のＰＭ３０の構成を示すブロック図。

【図３】図２中のフラッシュメモリ３５の記憶領域のメモリマップの一例を示す図。

【図４】ＯＰコードも含めて暗号化される秘匿Ｒ／Ｗ領域操作コマンドの形式を示す図。

【図５】秘匿Ｒ／Ｗ領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの一部を示す図。

【図６】秘匿Ｒ／Ｗ領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの他の一部を示す図。

【図７】秘匿Ｒ／Ｗ領域操作用の暗号化コマンドの送信から実行までの一連の動作を説明するためのフローチャートの残りを示す図。

【図８】秘匿Ｒ／Ｗ領域３５１の開始アドレスがＡＤ１の状態で、ＣＨＡＮＧＥコマンドによりＡＤ２（但し、

13

ＡＤ２＞ＡＤ１）に変更することが指定された場合の、当該ＣＨＡＮＧＥコマンド実行後のフラッシュメモリ３５のメモリマップを示す図。

【図９】パラメータだけが暗号化される秘匿Ｒ／Ｗ領域操作コマンドの形式を示す図。

【符号の説明】

１…ＰＣ（パーソナルコンピュータ）

１０…ＬＣＭ（コンテンツ利用管理システム、コンテンツ管理装置）

１１…セキュア・コンテンツ・サーバ

１２…ＰＤ　Ｉ／Ｆ部（送信手段）

１３…メディアＩ／Ｆ部（送信手段）

14

＊１４…ユーザＩ／Ｆ部

２０…ＰＤ（記録再生装置）

３０…ＰＭ（記憶媒体、記憶メディア）

３１…コントローラ

３２…コマンド復号部

３３…作業メモリ

３４…ＲＯＭ

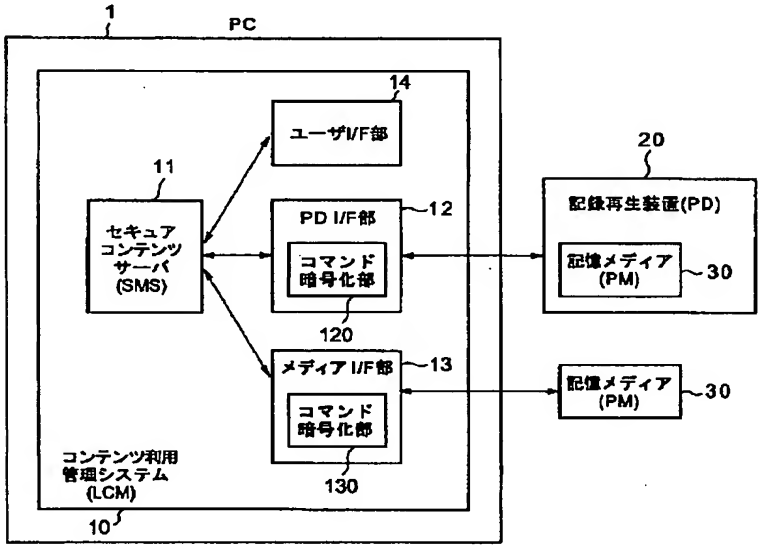
３５…フラッシュメモリ

１２０，１３０…コマンド暗号化部

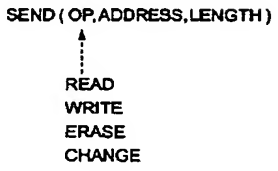
３５１…秘匿Ｒ／Ｗ領域

３５２…公開Ｒ／Ｗ領域

【図１】



【図４】



【図９】

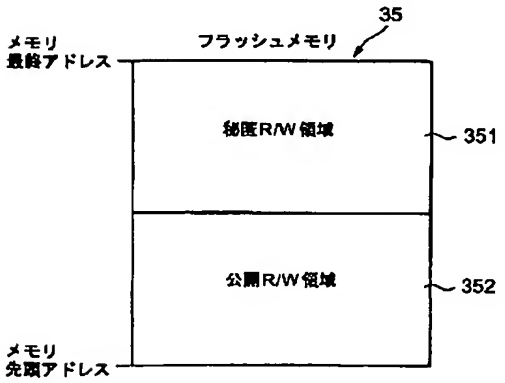
(a) READ (ADDRESS, LENGTH)

(b) WRITE (ADDRESS, LENGTH)

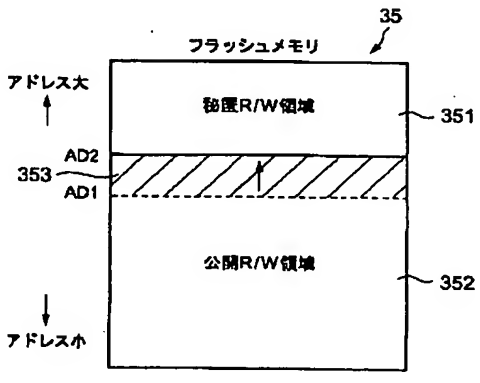
(c) ERASE (ADDRESS, LENGTH)

(d) CHANGE (ADDRESS, LENGTH)

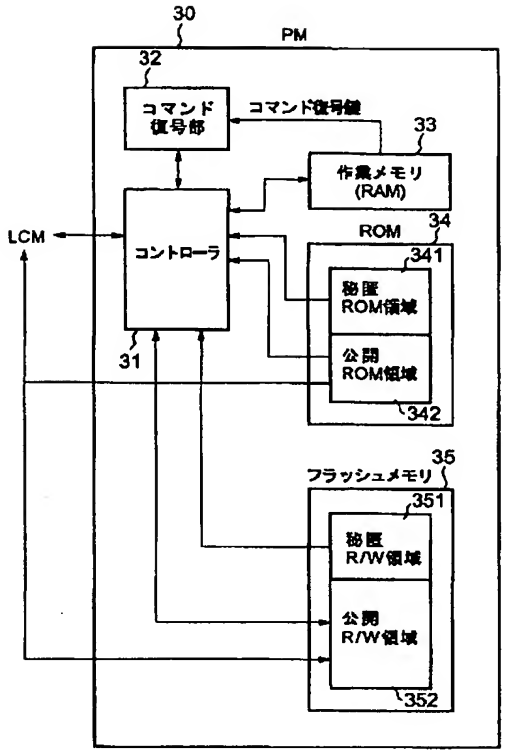
【図３】



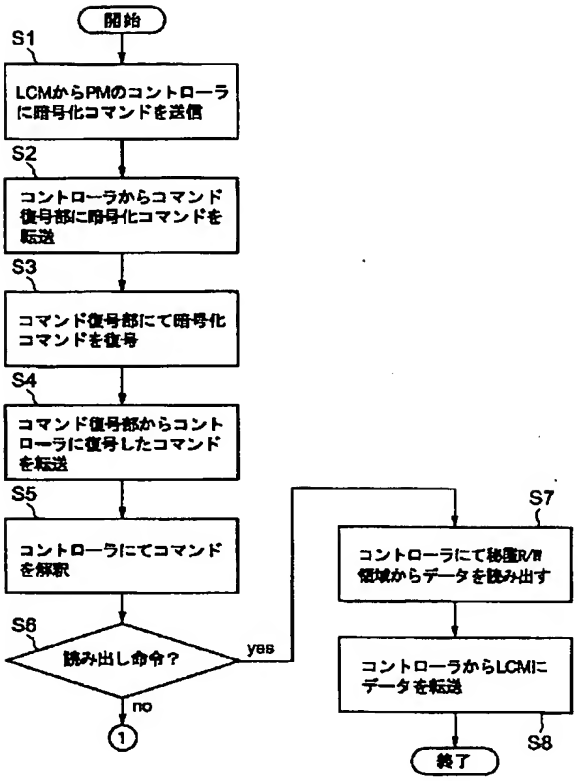
【図８】



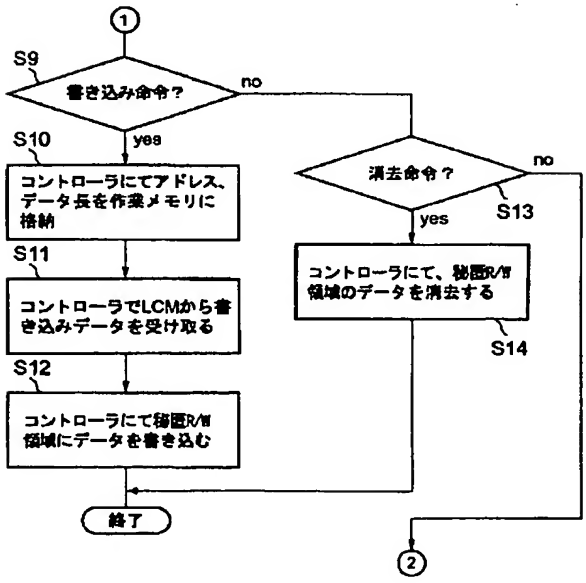
【図２】


30
PM
32
コマンド復号部
コマンド復号鍵
33
作業メモリ(RAM)
LCM
コントローラ
ROM
34
341
秘匿ROM領域
公開ROM領域
342
31
35
フラッシュメモリ
351
秘匿R/W領域
公開R/W領域
352

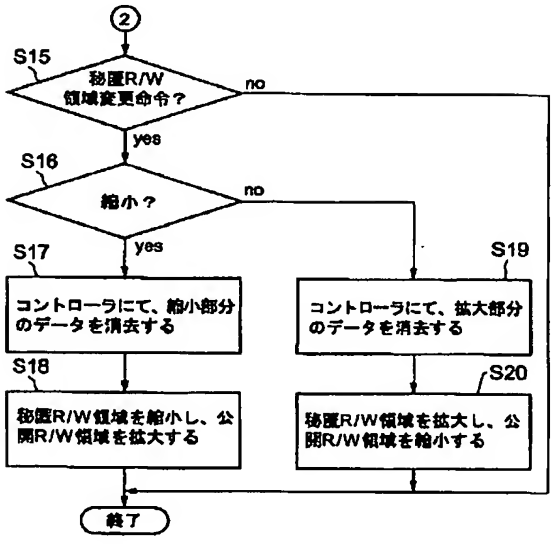
【図５】


開始
S1
LCMからPMのコントローラに暗号化コマンドを送信
S2
コントローラからコマンド復号部に暗号化コマンドを転送
S3
コマンド復号部にて暗号化コマンドを復号
S4
コマンド復号部からコントローラに復号したコマンドを転送
S5
コントローラにてコマンドを解釈
S6
読み出し命令？
yes
no
①
S7
コントローラにて秘匿R/W領域からデータを読み出す
コントローラからLCMにデータを転送
S8
終了

【図６】


①
S9
書き込み命令？
no
yes
S10
コントローラにてアドレス、データ長を作業メモリに格納
S11
コントローラでLCMから書き込みデータを受け取る
S12
コントローラにて秘匿R/W領域にデータを書き込む
終了
消去命令？
no
yes
S13
コントローラにて、秘匿R/W領域のデータを消去する
S14
②

【図７】


②
S15
秘匿R/W領域変更命令？
no
yes
S16
縮小？
no
yes
S17
コントローラにて、縮小部分のデータを消去する
S18
秘匿R/W領域を縮小し、公開R/W領域を拡大する
S19
コントローラにて、拡大部分のデータを消去する
S20
秘匿R/W領域を拡大し、公開R/W領域を縮小する
終了

フロントページの続き

Ｆターム(参考) 5B017 AA07 BA07 BB00 CA14
5C064 BA07 BB02 BC06 BC16 BC25
CA14 CB08 CC04
5J104 AA12 EA10 NA02